

# COOPER, SPONG & DAVIS

*Attorneys at Law*

200 High Street, Suite 500  
Post Office Box 1475  
Portsmouth, VA 23705-1475  
(757) 397-3481

Suffolk Executive Center  
424 Market Street, Suite 202  
Suffolk, VA 23434-5200  
(757) 539-1322

[www.cooperspong.com](http://www.cooperspong.com)

CLYDE W. COOPER (1933-1980)  
WILLIAM B. SPONG JR. (1920-1991)  
RICHARD J. DAVIS (1921-1999)  
ROBERT C. BARCLAY III (1972-2015)

ARNOLD H. LEON  
*RETIRED*

BRANCH H. DANIELS, JR.  
JOHN D. EURE, JR.\*  
DAVID R. LYNCH  
GREGORY M. POMJE  
SUSAN TAYLOR HANSEN  
ROBERT C. BARCLAY IV  
STEPHEN A. LEON  
MARY T. MORGAN  
ARTHUR C. BREDEMAYER  
EDWARD "TED" H. MILLER

\* OF COUNSEL

September 9, 2015

RECEIVED  
SEP 15 2015

## VIA USPS

Virginia Attorney General's Office  
Computer Crime Section  
900 E. Main Street  
Richmond, VA 23219

Computer Crime Section

Ladies and Gentlemen:

Pursuant to Virginia Code Section 18.2-186.6 I hereby notify you of a breach of the security of the computerized data system of the law firm of Cooper, Spong & Davis, P.C. which occurred during October 2014.

All Windows XP computers used by staff and attorneys and which were connected by our network had been replaced by April 14, 2014, the deadline for Microsoft's support of the XP. There was one exception. One new Windows 7 computer, one of two in our bookkeeping department, was not properly handling a certain software program. As a result, until that problem could be resolved, an XP computer had to be used to store personnel information, the username and password to Paychex, our payroll processor, and the password for accessing the firm's bank accounts.

Malware was discovered on that XP on October 10, 2014 and immediately quarantined. The XP was retired at the end of October 2014. A much later investigation showed that the malware infection had occurred on October 6, 2014.

The discovery of the malware infection on October 10, 2014 occurred because of a fraudulent attempt by someone to wire funds from the firm's operating bank account. Immediately after that failed attempt, Computer Solutions Group ("CSG"), the firm's outside IT provider, was called to investigate. Different malware detection software was run by CSG and this firm's office manager. One of those programs discovered the malware. There was no reason to suspect a breach of confidential personnel information. Only the bank password appeared to be the target.

Months later, during March 2015, it was realized that two firm employees had fraudulent tax returns filed in their name with the federal government. A firm meeting was called on March 16, 2015 to inform everyone of the situation. All former employees who had worked for the firm in 2014 and received W-2s from the firm were notified by telephone. A second firm meeting was held on March 31, 2015, to update everyone on our and CSG's investigation. This firm also reported the breach to the Portsmouth Police Department.

September 8, 2015

Page 2

Attached to this letter as Exhibit A is a letter signed by Jeff Carpenter of CSG confirming CGS's analysis and conclusions of how the breach occurred and what information was exposed.

Note that employee census data from 2003 through the time of the breach was stored in the XP's C-drive. The 2003 through 2013 censuses did not contain the then employees' home addresses. The information accessed may have included names, dates of birth, and Social Security numbers for employees listed on those censuses. That information as well as home addresses of this firm's employees and former employees who had worked during the calendar year of 2014 may have been accessed. The username and password to Paychex may have been obtained in order to get taxable wages and federal withholding information. The number of Virginia residents affected by the breach was forty-nine.

Attached to this letter as Exhibit B is a sample of the notification letter sent to the affected parties.

No client information was exposed by the breach. To this firm's knowledge, twelve false tax returns were fraudulently filed with the IRS for employees of this firm. There have been no reports of any fraudulent tax returns filed in the names of former employees. No former employees or current employees have reported any other difficulties which might be connected to the October 2014 breach.

If you need additional information or wish to discuss this matter, please contact Gregory M. Pomije, Esq. by mail at this address, by telephone at 757-397-3481, or by email (preferably) at [gpomije@portslaw.com](mailto:gpomije@portslaw.com). I remain

Very truly yours,

A handwritten signature in black ink, appearing to read "David R. Tynch", with a long horizontal flourish extending to the right.

David R. Tynch  
President,  
Cooper, Spong & Davis, P.C.

Exhibit A

## COOPER, SPONG & DAVIS

BRANCH H. DANIELS, JR.  
JOHN D. EURE, JR. \*  
DAVID R. TYNCH  
GREGORY M. POMJE  
SUSAN TAYLOR HANSEN  
ROBERT C. BARCLAY IV  
C. GERARD THOMPSON  
STEPHEN A. LEON  
MARY T. MORGAN  
ARTHUR C. BREDEMAYER  
EDWARD "TED" H. MILLER

\* OF COUNSEL

*Attorneys at Law*  
200 High Street, Suite 500  
Post Office Box 1475  
Portsmouth, VA 23705-1475  
(757) 397-3481

Suffolk Executive Center  
424 Market Street, Suite 202  
Suffolk, VA 23434-5200  
(757) 539-1322

[www.cooperspong.com](http://www.cooperspong.com)

CLYDE W. COOPER (1893-1980)  
WILLIAM B. SPONG, JR. (1920-1997)  
RICHARD J. DAVIS (1921-1999)

ROBERT C. BARCLAY III  
RETIRED

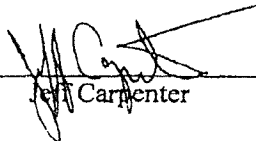
ARNOLD H. LEON  
RETIRED

March 24, 2015

To: Jeff Carpenter  
Computer Solutions Group

This will confirm our conversation through a telephone conference call with Jeff Carpenter of Computer Solutions Group ("CSG") on March 24, 2015 regarding data breach on one of the computers at Cooper, Spong & Davis. Jeff provided his analysis and conclusions as follows:

- One Windows XP was infected on October 6, 2014 at 10:21 a.m. by a malware (papras). The XP in question had been utilized by
- The probable virus was a password stealing malware. It digs into the C drive of the computer and finds passwords to websites visited during and prior to the period of infection. Malware also has a key logging capability exposing keyboard strokes with a potential for both user names and passwords being stolen.
- Paychex and TowneBank websites were likely visited during the infection period and it is assumed that those passwords were stolen. Malware found can also access files in the C drive. Employee Census files are saved in the C drive of the XP.
- No client information is kept or stored in the C drive. This malware is not capable of reaching into specialized and non-standard programs such as JST, or Perfect Law. Nor is this malware capable of migrating to another workstation or a network server.
- The most recent anti-virus scan on all workstations at Cooper, Spong & Davis, P. C. was run on March 16, and 17, 2015 and did not reveal any presence of virus or malware. In addition, all workstations are running an updated anti-virus software in the background in real time.
- The subject XP became free of malware on October 10, 2014 after Malware Bytes was run.
- Jeff made several recommendations to tighten up cyber security namely: Reviewing and tightening filtering security with Mailwatch; Check into UpRiver or Barracuda (similar email filtering programs); Purchase a new and updated Sonic Wall; Install Security Windows Patch monthly on all workstations; and a possible Vulnerability Monitoring Program that will scan for viruses. (Jeff has to do additional research on this program.)

  
Jeff Carpenter

4-2-15  
date

Exhibit B

## COOPER, SPONG & DAVIS

*Attorneys at Law*

200 High Street, Suite 500  
Post Office Box 1475  
Portsmouth, VA 23705-1475  
(757) 397-3481

CLYDE W. COOPER (1913-1994)  
WILLIAM A. SPONG, JR. (1925-1997)  
RICHARD J. DAVIS (1921-1974)  
ROBERT C. BARCLAY III (1912-1971)

BRANCH H. DANIELS, JR.  
JOHN D. EURE, JR.\*  
DAVID R. TYNCH  
GREGORY M. POMUE  
NIGAN TAYLOR HANSEN  
ROBERT C. BARCLAY IV  
STEPHEN A. LEON  
MARY T. MORGAN  
ARTHUR C. BRIDGEMeyer  
EDWARD "TED" H. MILLER

\*OF COUNSEL

Suffolk Executive Center  
424 Market Street, Suite 202  
Suffolk, VA 23434-5200  
(757) 539-1322

[www.cooperspong.com](http://www.cooperspong.com)

ARNOLD H. LEVY  
ATTORNEY

August 25, 2015

VIA HAND-DELIVERED

### NOTICE

Dear

We have eleven (11) employees in our firm who had fraudulent 2014 tax returns filed on their behalf earlier this year. We have reason to believe that the filing of these fraudulent tax returns was linked to a malware infection of an XP computer that stored personnel information and the user name and password to Paychex, our payroll processor. Later investigation showed that the malware infection occurred on October 6, 2014. The malware was discovered and then quarantined on October 10, 2014. The XP computer was retired at the end of October 2014.

October's search for a possible malware infection occurred because of a fraudulent attempt by someone to wire funds from the firm's operating bank account. Immediately after that failed attempt, Computer Solutions Group ("CSG"), the firm's outside IT provider, was called in to investigate. Different malware detection software was run by CSG and the firm's office manager. It was one of those programs that discovered the malware on October 10, 2014. There was no reason to suspect a breach of confidential personnel information, but only the bank password breach. Once the filing of the fraudulent employee tax returns became known, the firm realized more investigation was needed.

### **Information Accessed**

The information accessed may have included names, dates of birth, Social Security numbers, and home addresses of Cooper, Spong & Davis, P. C. employees and former employees. In addition, the user name and password to Paychex, our payroll processor, may have been used to obtain taxable wages and federal withholding information. It appears doubtful that the hacker or hackers wanted information about former employees who left Cooper, Spong & Davis, P.C. prior to the 2014 calendar year since information needed to be current for the filing of tax returns for the 2014 taxable year. However, employee censuses going back to 2005 containing certain employee information was on the hard drive of the infected XP computer, and that is why this letter is being sent to anyone who worked at this firm from 2003 through 2013 as

well. The 2003 through 2013 employee censuses on the hard drive did not contain employees' home addresses.

### **Action Taken**

As soon as we were informed of the 2<sup>nd</sup> fraudulent tax return filed, a firm meeting was called on March 16, 2015 to inform everyone of the situation. All former employees who worked for the firm in 2014 and received W2s from the firm were notified by telephone. A second firm meeting was held on March 31, 2015 to update everyone of the result of our and CSG's investigation. We advised everyone on how to place a credit fraud alert on their credit profile by using one of the nationwide Credit Bureaus. We provided the IRS Identity Theft Number (1-800-908-4490) and encouraged everyone to call. We also reported the identity theft incidents to the Portsmouth Police Department who sent several police officers on March 23, 2015 to take our employees' written statements.

### **Fraud Prevention Tips**

We want to ensure that you have the knowledge on how to guard against identity theft and fraud. We strongly encourage everyone to add a fraud alert to your credit report to help protect your credit information. A fraud alert can make it difficult for someone to get credit under your name because it requires creditors to follow certain procedures. These procedures can include the creditor making an independent call to you while credit application is being processed and your having to prove your identity by answering questions that are on your credit file. Please note that a fraud alert in some instances may also delay your ability to obtain credit. In addition, you may also be able to put a security freeze on your credit file by calling any one of the credit bureaus.

You can report suspected identity thefts to the Federal Trade Commission or the Virginia State Attorney General's Office. The Internal Revenue Service has excellent information on Identity theft which can be accessed using the link <http://www.irs.gov/Individuals/Identity-Protection>.

In addition, if you are member of the AAA Auto Club, we recommend that you sign up for their free Daily Credit Monitoring service.

We advise everyone to remain vigilant by reviewing account statements and monitoring free credit reports.

### **Credit Bureau Information and Important Websites**

Equifax - P. O. Box 740241, Atlanta, GA 30374-0241  
Phone Number 1-800-685-1111  
equifax.com

Experian - P. O. Box 9532, Allen, TX 75013  
Phone Number - 1-888-397-3742  
experian.com

TransUnion -- P. O. Box 2000, Chester, PA 19022  
Phone Number 1-800-916-8800  
transunion.com

IRS Identity Theft Hotline -- 1-800-908-4490

Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
[www.ftc.gov](http://www.ftc.gov) or call 1-877-ID-THEFT

If you have any questions or require assistance regarding this matter, please contact  
Eugenia E. Alindogan at (757) 391-3124.

Very truly yours,

A handwritten signature in black ink, appearing to read "D. Tynch". The signature is written in a cursive, flowing style.

David R. Tynch  
President  
Cooper, Spong & Davis, P.C.